

UNITED STATES DISTRICT COURT

for the
Southern District of OhioFILED
RICHARD W. NAGEL
CLERK OF COURT

2018 APR 17 AM 10:12

U.S. DISTRICT COURT
SOUTHERN DIST. OHIO
WESTERN DIV. DAYTONIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)APPLE IPHONE MODEL A1778, LOCATED IN
EVIDENCE LOCKER, U.S. SECRET SERVICE, ROOM
811, 200 W. SECOND ST, DAYTON, OH 45402

Case No.

3:18mj316

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):
APPLE IPHONE MODEL A1778, IC: 579C-E3091A LOCATED IN EVIDENCE LOCKER, U.S. SECRET SERVICE, ROOM 811, 200 W. SECOND ST, DAYTON, OH 45402

located in the _____ District of _____, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section

Offense Description

SEE ATTACHMENT C

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

☒ Continued on the attached sheet.

☐ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date: 4/17/18City and state: DAYTON, OHIO

Jennifer M. Tron
 Applicant's signature
 JENNIFER M. TRON, SA U.S. SECRET SERVICE

Michael J. Newman
 Printed name and title
 Judge's signature
 MICHAEL J. NEWMAN U.S. MAGISTRATE JUDGE
 Printed name and title

ATTACHMENT C

18 U.S.C. § 1028	Fraud and related activity in connection with Identification documents
18 U.S.C. § 1028A	Aggravated identity theft
18 U.S.C. § 1029	Access device fraud
18 U.S.C. § 1030	Fraud and related activity in connection with Computers
18 U.S.C. § 1341	Fraud
18 U.S.C. § 1343	Wire fraud
18 U.S.C. § 371	Conspiracy
18 U.S.C. § 1349	Conspiracy to commit fraud

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF
APPLE iPHONE X, APPLE iPHONE
MODEL A1778, IC: 579C-E3091A, AND
APPLE iPHONE MODEL A1784, IC: 579C-
E3092A CURRENTLY LOCATED AT
UNITED STATES SECRET SERVICE,
DAYTON RESIDENT OFFICE, 200 W.
SECOND STREET, SUITE 811, DAYTON,
OHIO 45402

Case No. _____

**AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER
RULE 41 FOR A WARRANT TO SEARCH AND SEIZE**

I, Jennifer M. Tron, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I submit this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for search warrants authorizing the forensic examination and extraction of electronically stored data and information, (specifically described and listed in **Attachment B** of this affidavit) which are contained in certain property, to wit: electronic devices, which are specifically described and listed in **Attachment A** of this affidavit. All of the subject electronic devices are currently in the possession of law enforcement authorities. This application is a renewal of a previous unexecuted Search Warrant issued by United States Magistrate Judge Sharon L. Ovington on March 22, 2018, which time lapsed on or about April 5, 2018.

2. I am a Special Agent with the United States Secret Service (USSS), and have been so employed since March 1999. I am currently assigned to the Dayton Resident Office. I have received extensive training in the criminal investigation of a wide variety of white collar-

fraud related crimes to include: Identification Document Fraud, Aggravated Identity Fraud, Access Device Fraud, Fraud in Connection With Computers, Mail Fraud, Wire Fraud and Conspiracy in violation of Title 18 United States Code, Sections 1028, 1028A, 1029, 1030, 1341, 1343, 371 and 1349 respectively.

3. This affidavit is only intended to establish the existence of sufficient probable to justify the requested warrants, and does not set forth all the facts presently known by the investigation pending in this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The individual items of property desired to be searched are listed below. Each device is currently stored in a secure evidence locker located in the U.S. Secret Service, Dayton Resident Office, 200 W. Second Street, Suite 811, Dayton, Ohio 45402.

- a. Apple iPhone X,
- b. Apple iPhone Model A1778, IC: 579C-E3091A, and
- c. Apple iPhone Model A1784, IC: 579C-E3092A.

5. The applied-for search warrants would authorize the forensic examination of each the above listed Devices described in **Attachment A**, for the purpose of identifying and reviewing electronically stored data more particularly described in **Attachment B**.

PROBABLE CAUSE

6. The following information is personally known to your Affiant, or was reported to her by other law enforcement officers involved with, and otherwise knowledgeable of the facts and circumstances associated with subject case.

7. On the afternoon of January 25, 2018, your Affiant was contacted by Agent Rich Miller, a Task Force Officer assigned to the Miami Valley Bulk Smuggling Task Force. Agent Miller advised that he had been conducting surveillance operations at or near a Dayton area hotel located in the Miller Lane area. During the course of this operation, he observed suspicious

activity associated with an occupant of a Nissan Armada automobile bearing Florida license plate # 166-YTH that was then parked at a nearby gas station. While at this gas station, Agent Miller observed the initial suspect (later identified to be Leonardo Wolf Targino (hereinafter referred to as "**TARGINO**") leaving said vehicle to enter the gas station. Agent Miller observed **TARGINO** use a credit card to pay \$50.00 for gas purchased from Pump #5. Agent Miller thereafter observed **TARGINO** attempt to use numerous credit cards at an adjacent ATM machine. Agent Miller specifically observed **TARGINO** repeatedly reference his cell phone after inserting various cards into the ATM machine. **TARGINO** was observed attempting to complete multiple transactions using multiple cards. **TARGINO** thereafter returned to the said Nissan Armada. Soon thereafter, a second vehicle, to wit: a Chevy Tahoe bearing Florida license plate # 952-LZD approached the Nissan Armada. A total of five (5) individuals who had occupied both said vehicles exited their respective cars and engaged in conversation in a language other than English. Eventually all of the five individuals re-entered their respective vehicles before departing to a nearby steak restaurant. Agent Miller followed the two (2) suspect vehicles to the restaurant. The five (5) suspects entered the restaurant parking lot. While the five individuals were inside the restaurant, Agent Miller ran the two (2) subject vehicle license plates in various law enforcement data bases. As a result, he learned both vehicles were rented. Agent Miller proceeded to contact the rental car company for the Nissan Armada and learned that an individual identified as "Felipe Mello" rented it in Chicago, IL. Additional law enforcement data base checks revealed that there was an active New York State Police "alert" posted for a "Felipe Pinheiro Mello" for questioning on suspected fraudulent credit card purchases in Genesee County, NY. Upon gathering this information, Agent Miller contacted the USSS Dayton Residence for further assistance and guidance in this matter.

8. Your Affiant and USSS Dayton Resident RAIC Kevin Dye, immediately responded to the said restaurant parking lot to provide assistance in the investigation. The four

male suspects were identified as **TARGINO**, Diego M. DaCosta (hereinafter referred to as “**DACOSTA**”), Ricardo Carlos De Andrade (hereinafter referred to as “**ANDRADE**”) and Sandro Lopes Trancoso DaSilva (hereinafter referred to as “**SILVA**”). A female juvenile was also identified to have been a passenger in the Nissan Armada. This person is identified with the initials “**MBM**”. All five (5) occupants of the two (2) suspect vehicles were determined to be natives of Brazil. **DACOSTA** was the only vehicle occupant determined to be an authorized permanent U.S. resident. According to information provided by ICE officials, he apparently has lawfully resided in the U.S. since age 10.

9. After law enforcement officials established the identities of the five occupants, multiple counterfeit credit cards bearing the names “Felipe Mello” and “Richard Martins” were located on or near the persons of **DACOSTA**, **TARGINO**, **ANDRADE**, and **SILVA**. RAIC Dye verbally advised **DACOSTA** of his *Miranda* Rights using the English language. **DACOSTA** acknowledged that he understood both the English language and his legal rights. He indicated he was willing to answer questions and cooperate with this investigation. He further stated that the other four (4) individuals only spoke Portuguese and were not otherwise fluent in English. **DACOSTA** further indicated to Agent Miller that the Spanish language is very similar to Portuguese. He further volunteered to assist law enforcement authorities in communicating with **TARGINO**, **ANDRADE**, and **SILVA** in Portuguese.

10. **TARGINO** was identified as the driver of Nissan Armada. **ANDRADE** was identified as the driver of the Chevy Tahoe. Agent Miller provided a verbal Spanish translation of the Consent to Search Form and compared it to the Portuguese translation **DACOSTA** provided. **DACOSTA** translated the Consent to Search Form for both rental vehicles from English into Portuguese. As a result, both **TARGINO** and **ANDRADE** indicated their

respective understanding of the consent forms, and both willingly agreed to sign their individual written consent search forms. Both vehicles were impounded in accordance with established law enforcement policies. Both vehicles were searched pursuant to the written consents provided by both **TARGINO** and **ANDRADE** and the inventory search procedures.

11. These searches resulted in the discovery and seizure of: three (3) Laptop computers, a magnetic stripe credit card reader/writer/encoder, a MSR Mini used to skim and store credit card account numbers, and more than 400 counterfeit credit cards. Other items recovered from the Chevy Tahoe included: ATM skimmers, multiple pinhole cameras, ATM card reader overlays, and various tools and materials used to alter ATMs.

12. The said four (4) male suspects and the juvenile female were thereafter transported to the Butler Township Police Department in Dayton, OH. RAIC Dye, and your Affiant responded to the Butler Township Police Department.

13. Upon arriving at the Butler Township Police Department, RAIC Kevin Dye, Det. Jason Leslie of the Butler Township Police Dept., and your Affiant interviewed **DACOSTA**. Prior to questioning, **DACOSTA** was advised of his *Miranda* Rights both verbally and in writing via a SSF 1737B. **DACOSTA** acknowledged and waived his legal rights. **DACOSTA** advised that he speaks and reads English fluently. **DACOSTA** agreed to speak with investigators and provided the following information.

14. **DACOSTA** stated that he moved to the United States with his family when he was 10 years of age. **DACOSTA** further stated that he was educated at the University of Massachusetts. Upon graduation, he worked in the investment banking business until he lost his job a couple of years ago. After his wife divorced him he claimed that he lost everything. As such, approximately six (6) months ago he started working in Florida for a fraudulent credit card

business. He stated that the guys who ran this illicit business paid him 25% of the illicit proceeds he generated during the three (3) months that he worked for them.

15. Approximately three (3) months ago, **DACOSTA** met **TARGINO**. **TARGINO** offered **DACOSTA** a 50% split of the illicit proceeds of his fraud scheme so he started working with **TARGINO**.

16. **DACOSTA** stated that he had begun traveling with **TARGINO** and the 17-year old juvenile female **MBM**. She had flown from Brazil to Fort Lauderdale, FL with her parent's consent in order to meet **TARGINO**, who is her boyfriend. He further stated that the three of them began their automobile trek from Florida the last week of December. He claimed that they stayed at the Addington Hotel which is located at 36th and Lexington Ave. in New York. While in New York City, they engaged in a shopping spree.

17. On January 4th or 5th, they departed New York City for Buffalo, NY. **DACOSTA** advised that they stayed at a Hyatt Hotel in Buffalo and another hotel which he described as Italian but could not remember a name. He claimed that they stayed three (3) days in each hotel location. During their stay in the Buffalo area, they shopped for electronics and clothing.

18. At some point prior to departing Buffalo, **DACOSTA** advised that **TARGINO** arranged for them to meet **ANDRADE** and **DESILVA** in Cleveland, OH. As such, they proceeded to Cleveland, OH where they stayed at a Doubletree Hotel (unknown address) and attended a Cleveland Cavaliers NBA basketball game.

19. **DACOSTA** further advised that the credit card fraud scheme consisted in-part of the group purchasing counterfeit credit cards for \$80.00 each. The plastic cards would be sent to them via FedEx from associates located in Florida. **DACOSTA** stated that they received counterfeit cards at two (2) different FedEx locations (one in NY and one in Cleveland) during

the trip. He additionally stated that the conspirators have manufactured and sold counterfeit Brazilian identification cards/documents.

20. **DACOSTA** stated that “**MBM**” never made any illicit purchases and did not have any counterfeit cards provided to her during their travels.

21. RAIC Dye next interviewed **TARGINO**. This interview was conducted with the telephonic assistance of a Portuguese Interpreter named Gabrielle Sago (#251358). Prior to questioning, **TARGINO** was advised of his *Miranda* Rights which was witnessed by Det. Leslie. **TARGINO** acknowledged understanding his legal rights verbally and in writing via a SSF 1737B. He agreed to answer questions and cooperate with the investigation. The following is a summary of **TARGINO**’s translated verbal statement he provided to investigators.

22. **TARGINO** corroborated the key details of the group’s travels and fraud scheme previously provided by **DACOSTA**. He additionally added that he paid \$80.00 for each counterfeit credit card provided by unidentified associates based in Ft. Lauderdale, FL. He further stated that he had been engaged in unlawful counterfeit credit card activities for approximately six months, since his father had been arrested.

23. **TARGINO** self-identified himself as an “overstay” on a U.S. visitor visa. **TARGINO** further stated that during his most recent trip to New York, Buffalo, Chicago and Cleveland, he had purchased approximately 330 counterfeit credit cards, which were shipped to him from Florida associates. These counterfeit credit cards were received in two separate FedEx shipments.

24. **TARGINO** estimated that he had made between \$5,000.00 - \$6,000.00 during the trip. He also stated that during this current trip, he split all his cash earnings 50/50 with **DACOSTA**.

25. Law enforcement authorities found a National Car Rental receipt located inside the Nissan Armada. This receipt contained the alias name, “Felipe Mello”, as the individual who rented the vehicle on January 22, 2018 in Chicago, IL. This vehicle was rented using a Master Card with an account number ending in 0652. A Master Card credit card bearing said account number and the embossed name of “Felipe Mello” and was found in **DACOSTA**’s wallet.

26. All of the said seized electronic devices were transported to USSS Dayton Resident Office, located at 200 West Second Street, Dayton, Ohio, 45402, where they have remained in secure storage until the present.

27. On February 14, 2018, your Affiant confirmed that said Chevy Tahoe bearing Florida license plate # 952-LZD was rented at the Miami Airport on January 6, 2018 by a “Ricardo De Andrade.” **ANDRADE** paid for this vehicle rental with a Visa credit card with an account number ending in 4823. This credit card was located by law enforcement authorities inside the said Nissan Armada bearing Florida license plate # 166-YTH. This credit card bears the embossed name, “Felipe Mello.”

28. Further investigation conducted by your Affiant, with the assistance of USSS Special Agents located in resident offices located in Miami, FL; West Palm Beach, FL; Orlando, FL; Baltimore, MD; Savannah, GA; New York, NY; Buffalo, NY; Cleveland, OH; Chicago, IL; Charlotte, NC; Canada, Mexico, and Brazil, has confirmed the existence of a nation-wide fraud network of Brazilian Nationals based out of South Florida. This conspiracy has been involved in illicit ATM skimming operations and access device fraud activities involving counterfeit credit cards.

29. While the USSS in all likelihood possesses sufficient legal authority to proceed with the forensic examination of each of the said electronic devices, out of an extreme abundance

of caution, your Affiant respectfully seeks additional and specific search warrants for each of the listed devices. This action is taken to ensure such examinations fully comply with all possible Fourth Amendment and other legal requirements.

30. Based upon my prior law enforcement training and experience, your Affiant feels confident all of the electronic devices have been stored and maintained in a manner that ensure their respective contents have remained, to the maximum extent possible, in substantially the same state and condition they were when they first came into the possession of the USSS.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

31. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

32. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has

used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

33. *Forensic evidence.* As further described in **Attachment B**, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other

information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device to obtain unauthorized access to a victim electronic device over the Internet, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

34. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

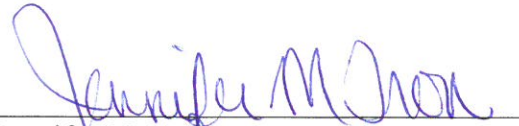
35. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

36. I submit that the facts set forth in this affidavit establish sufficient probable cause to support the issuance of individual search warrants authorizing the forensic examination of

each of the electronic devices listed and described in **Attachment A**, seeking the items of evidence and electronic data described in **Attachment B**.

37. It is respectfully requested that this application be ordered sealed by this Honorable Court until further order of the Court.



Jennifer M. Tron
Senior Special Agent
United States Secret Service

Subscribed and sworn to before me
this 17th day of April, 2018.



MICHAEL J. NEWMAN
UNITED STATES MAGISTRATE JUDGE

